

# An attack against the Helios election system that violates eligibility

Maxime Meyer and Ben Smyth

Mathematical and Algorithmic Sciences Lab,  
Huawei Technologies Co. Ltd., France

December 14, 2016

## Abstract

Election systems must ensure that representatives are chosen by voters. Moreover, each voter should have equal influence. Traditionally, this has been achieved by permitting voters to cast at most one ballot. More recently, this has been achieved by counting the last ballot cast by each voter. We show that the Helios election system fails to achieve this, because an adversary can cause a ballot other than a voter's last to be counted. Moreover, we show how the adversary can choose the contents of such ballots, thus the adversary can unduly influence the selection of representatives.

## 1 Introduction

An election is a decision-making procedure to choose representatives [14, 18, 9, 3]. Choices are made by voters, and this must be ensured by election systems, as prescribed by the United Nations [25, Article 21], the Organization for Security and Cooperation in Europe [16, Paragraph 7.3], and the Organization of American States [15, Article 23]. These organisations also prescribe that election systems must ensure that voters have equal influence in the decision [25, 16, 15]. This has led to the emergence of the following requirement.

- Eligibility. Choices are made by voters, and only the last choice of each voter has influence.

Eligibility ensures that non-voters cannot (directly) influence the decision.<sup>1</sup> For instance, national elections typically require that voters are citizens of the nation, thus eligibility forbids influence from foreign citizens. Eligibility also ensures that each voter can contribute at most one choice, hence, voters have equal

---

<sup>1</sup>We concede that non-voters may indirectly influence the decision, e.g., non-voters may coerce voters to influence the decision.

influence. Moreover, eligibility enables voters to change their choices, which provides flexibility, and aids education (since voters can “*ask the help of anyone for submitting a random ballot, and then re-voting privately afterwards*” [1, §3.3]). In addition, for verifiable elections [6, 11, 13, 22, 10], eligibility is useful to aid recovery from failure (since voters can “*vote, verify, and revote until verification succeeds*” [2, §1]). Eligibility can be assured cryptographically (cf. eligibility verifiability [22]) or enforced by a trusted party [22, §2.2.3]. In both cases, someone must be able to check that choices were made by voters, hence, choices must be authenticated.

We analyse Helios [1]: an open-source, web-based election system,<sup>2</sup> which has been used by the International Association of Cryptologic Research (IACR), the ACM, the Catholic University of Louvain, and Princeton University [17]. Helios uses a trusted party for authentication and we show that the authentication mechanism is insufficient to ensure eligibility.

## 2 Analysis of Helios

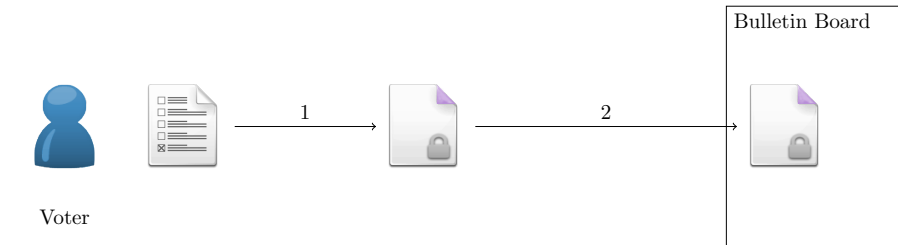
### 2.1 Protocol description

An execution of Helios (Figure 1) proceeds as follows. First, a voter casts a ballot for their choice: the voter encrypts their choice (1) and sends their encrypted choice to the bulletin board (2). Secondly, the voter authenticates their encrypted choice to the bulletin board, to prove that they are indeed a voter. The authentication process is reliant on a trusted party and it proceeds as follows. The voter authenticates to a trusted party (3), the trusted party generates a token for the voter (4), the voter sends the token to the bulletin board (5), and the bulletin board relays the token to the trusted party (6). The trusted party checks whether the token is valid and notifies the bulletin board of the token’s validity (7). If the token is valid, then the bulletin board accepts the voter’s encrypted choice. Hence, the bulletin board contains the voter’s authenticated encrypted ballot. In addition, the bulletin board discards any encrypted choice previously accepted for that voter, which is intended to ensure that only the last choice of each voter has influence. Finally, the bulletin board homomorphically combines the accepted encrypted choices (8), the administrator decrypts the homomorphic combination (9), and the bulletin board reveals those decrypted choices (10).

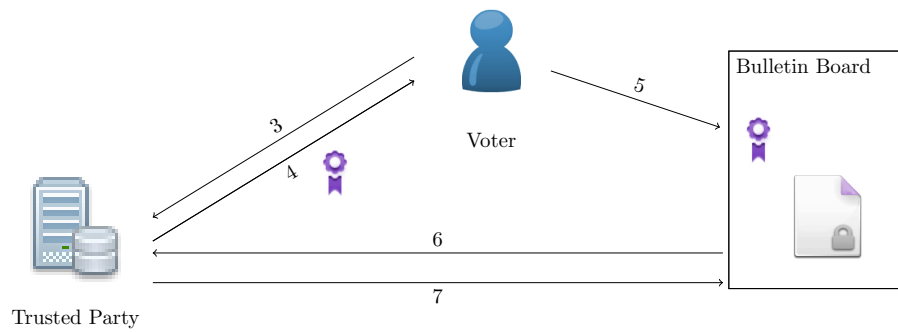
Helios is intended to satisfy eligibility, because encrypted choices are only accepted by the bulletin board when accompanied by a token authenticating the voter that constructed the encrypted choice. And, upon acceptance, the bulletin board discards any encrypted choice previously accepted for that voter. Unfortunately, this is insufficient.

---

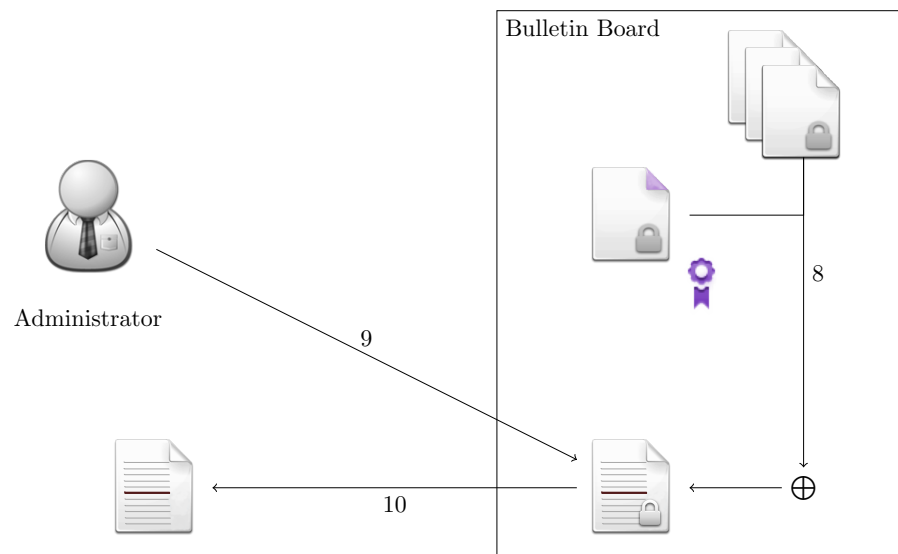
<sup>2</sup><https://vote.heliosvoting.org>, accessed 19 Aug 2015.



(a) Casting a ballot



(b) Authenticating the ballot



(c) Tallying

Figure 1: Helios protocol flow

## 2.2 Attack

The start of our attack corresponds to an honest execution: a voter casts a ballot for their choice, as per Figure 1a. The remaining steps (Figure 2) proceed as follows. First, the adversary intercepts a voter’s token: the voter authenticates to a trusted party (1), receives an authentication token (2), and sends the token to the bulletin board (3), but it is intercepted by the adversary (4).<sup>3</sup> (We indicate the relation between ballot and token by colouring the top right-hand corner of the ballot and the token in purple.) Thus, the bulletin board contains an unauthenticated encrypted choice and is awaiting an authentication token for that encrypted choice. Next, the attacker waits until the voter casts another encrypted choice (5), authenticates with a trusted party (6), receives a token (7), and sends the token to the bulletin board (8). (We indicate the relation between ballot and token using green colouring.) Thus, the bulletin board can authenticate the voter’s second ballot. Finally, the adversary releases the intercepted token and it is received by the bulletin board (9). Thus, the bulletin board will accept the voter’s first ballot, and discard the voter’s second ballot (10). Consequently, the voter’s first choice is tallied, rather than their second. Hence, eligibility is not satisfied, because only the last choice of the voter should have influence, which is not the case.

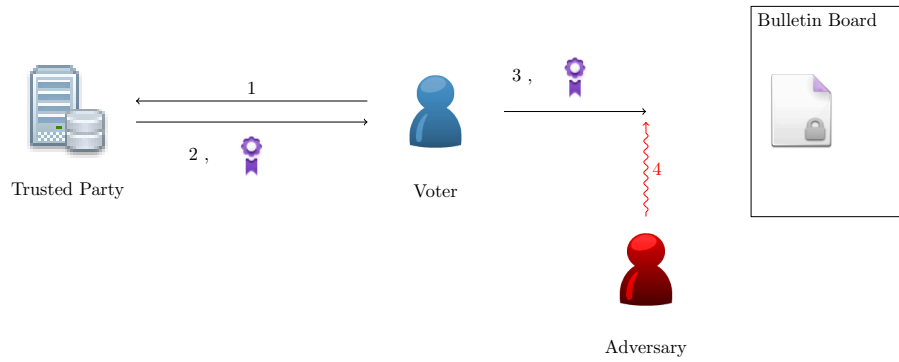
**Video demonstration.** Our attack is demonstrated in a supporting video [24].

## 2.3 Impact

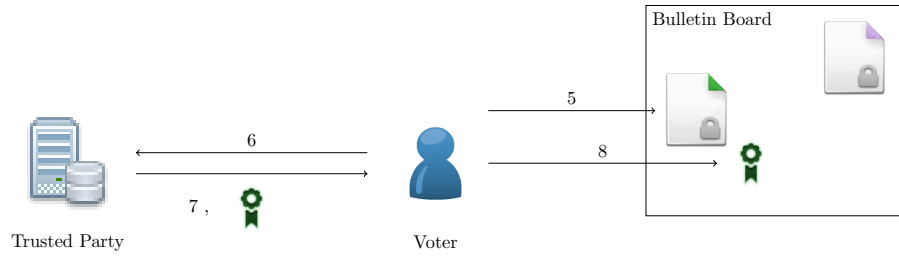
Let us now consider how an adversary might unduly influence an election’s outcome in settings where Helios is deployed in voting terminals located at poll stations. In such settings, a malicious election supervisor could offer to demonstrate the Helios system to a voter, under the guise of education. During the demonstration, the supervisor could suggest that the voter selects a particular choice. This should not cause suspicion, because Helios is intended to permit voters to change their choices. Once the voter casts the demonstration ballot, it could be intercepted, perhaps by a router in the polling station that the supervisor controls. After the demonstration, the supervisor could instruct the voter to re-vote in private. Once the voter leaves the poll station, the intercepted ballot could be released. Consequently, the supervisor’s choice is tallied, rather than the voter’s. We acknowledge that the voter can discover that this attack has taken place, by checking whether the bulletin board accepted their second encrypted choice (cf. individual verifiability [22, 11]). However, Helios does not provide *accountability* [12] – hence, the adversary’s actions cannot be attributed

---

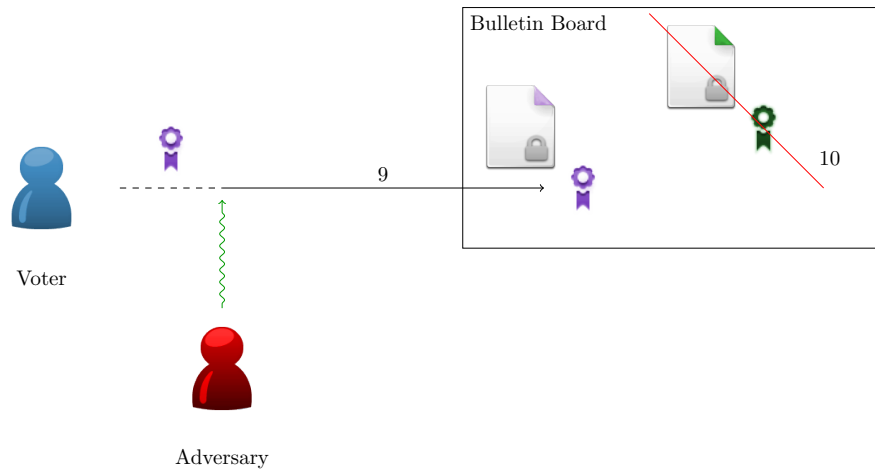
<sup>3</sup> An adversary can intercept packets even when they are encrypted. For example, packets sent over a TLS connection, i.e., encrypted packets, can be intercepted. Intercepting a TLS packet prevents further data from being received on *that* TLS connection (until the packet is released), but data may be received on other TLS connections, because TLS does not guarantee ordering of messages between connections. Hence, TLS does not prevent further communication between the voter and the bulletin board.



(a) Token interception



(b) Casting a second ballot



(c) Release intercepted token

Figure 2: Helios attack flow

to any party – and the voter is unable to convince the administrator that any malpractice has taken place.

## 2.4 Fixes

The attack can be prevented by timestamping authentication tokens, coupling the encrypted choice with a counter, or proving knowledge of earlier encrypted choices *à la* Clarkson, Chong & Myers [5, §3.3]. We favour timestamping authentication tokens, since the other approaches require the voter to maintain state. Moreover, we recommend that the authentication mechanism is further adapted to permit anyone to check the validity of authentication tokens, rather than just the bulletin board.

## 3 Related work

Smyth & Pironti [23] identify a flaw in Helios’s sign-out procedure which can be exploited by TLS truncation attacks to dupe voters into believing they have successfully signed-out, when they have not. Thus, an adversary can make a choice on the voter’s behalf from the terminal used by the voter, thereby violating eligibility. Beyond eligibility, malleability has been exploited to launch attacks against ballot secrecy [7, 21, 19, 8, 20] and verifiability [22], and unsound proofs of knowledge have been exploited to launch further attacks against verifiability [4].

## 4 Conclusion

We have shown that Helios does not satisfy eligibility, because an adversary can cause a ballot other than a voter’s last to be tallied. In particular, the adversary can intercept the authorization token associated with the ballot that the adversary wants tallied, wait until the voter has casts their last ballot, and then release the intercepted token. The released token causes the bulletin board to accept the ballot that the adversary wants tallied, and to discard the voter’s last ballot. Thus, eligibility is not satisfied. We have also shown that an adversary can unduly influence election outcomes. In particular, the adversary can exploit the educational needs of voters to cast a ballot for the adversary’s choice, and cause that ballot to be tallied rather than the voter’s last, as we have explained.

## Acknowledgments

We thank Elizabeth Quaglia and Susan Thomson for discussions that helped improve this paper.

Smyth’s work was largely performed at INRIA, with support from the European Research Council under the European Union’s Seventh Framework Programme (FP7/2007-2013) / ERC project *CRYSP* (259639).

## References

- [1] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios. In *EVT/WOTE’09*. USENIX, 2009.
- [2] Ben Adida and C. Andrew Neff. Ballot casting assurance. In *EVT’06*. USENIX, 2006.
- [3] R. Michael Alvarez and Thad E. Hall. *Electronic Elections: The Perils and Promises of Digital Democracy*. Princeton University Press, 2010.
- [4] David Bernhard, Olivier Pereira, and Bogdan Warinschi. How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In *ASIACRYPT’12*, volume 7658 of *LNCS*, pages 626–643. Springer, 2012.
- [5] Michael R. Clarkson, Stephen Chong, and Andrew C. Myers. Civitas: Toward a Secure Voting System. In *SE’08*, pages 354–368. IEEE, 2008.
- [6] Josh Daniel Cohen and Michael J. Fischer. A Robust and Verifiable Cryptographically Secure Election Scheme. In *FOCS’85*, pages 372–382. IEEE, 1985.
- [7] Véronique Cortier and Ben Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. In *CSF’11*, pages 297–311. IEEE, 2011.
- [8] Véronique Cortier and Ben Smyth. Attacking and fixing Helios: An analysis of ballot secrecy. *Journal of Computer Security*, 21(1):89–148, 2013.
- [9] Andrew Gumbel. *Steal This Vote: Dirty Elections and the Rotten History of Democracy in America*. Nation Books, 2005.
- [10] Aggelos Kiayias, Thomas Zacharias, and Bingsheng Zhang. End-to-End Verifiable Elections in the Standard Model. In *EUROCRYPT’15*, volume 9057 of *LNCS*, pages 468–498. Springer, 2015.
- [11] Steve Kremer, Mark D. Ryan, and Ben Smyth. Election verifiability in electronic voting protocols. In *ESORICS’10*, volume 6345 of *LNCS*, pages 389–404. Springer, 2010.
- [12] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Accountability: Definition and relationship to verifiability. In *CCS’10*, pages 526–535. ACM, 2010.

- [13] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study. In *SE&P'11*, pages 538–553. IEEE, 2011.
- [14] Arend Lijphart and Bernard Grofman. *Choosing an electoral system: Issues and Alternatives*. Praeger, 1984.
- [15] American Convention on Human Rights, “Pact of San Jose, Costa Rica”, 1969.
- [16] Document of the Copenhagen Meeting of the Conference on the Human Dimension of the CSCE, 1990.
- [17] Olivier Pereira. Internet Voting with Helios. In *Real-World Electronic Voting: Design, Analysis and Deployment*, volume 8604, chapter 11. CRC, 2016.
- [18] Thomas Saalfeld. On Dogs and Whips: Recorded Votes. In *Parliaments and Majority Rule in Western Europe*, chapter 16. St. Martin’s Press, 1995.
- [19] Ben Smyth. Replay attacks that violate ballot secrecy in helios. Technical Report 2012/185, Cryptology ePrint Archive, 2012.
- [20] Ben Smyth. Secrecy and independence for election schemes. Technical Report 2015/942, Cryptology ePrint Archive, 2015.
- [21] Ben Smyth and Véronique Cortier. A note on replay attacks that violate privacy in electronic voting schemes. Technical Report RR-7643, INRIA, 2011.
- [22] Ben Smyth, Steven Frink, and Michael R. Clarkson. Election Verifiability: Cryptographic Definitions and an Analysis of Helios and JCJ. Technical Report 2015/233, Cryptology ePrint Archive, 2015.
- [23] Ben Smyth and Alfredo Pironti. Truncating TLS Connections to Violate Beliefs in Web Applications. In *WOOT'13*. USENIX Association, 2013.
- [24] Ben Smyth and Susan Thomson. Helios Re-voting Attack. YouTube video, linked from <https://bensmyth.com/publications/2016-attacking-eligibility-in-Helios/>, 2014.
- [25] Universal Declaration of Human Rights, 1948.